Mapping War, Peace and Terrorism in the Global Information Environment

Michael John-Hopkins

Senior Lecturer in Law; School of Law, Faculty of Humanities and Social Sciences, Oxford Brookes University, Headington Hill Hall, Oxford

john-hopkins@brookes.ac.uk

Abstract

This article outlines in general terms how the environment of 21st century transnational organised crime, terrorism and unconventional conflict is being shaped by information-related capabilities (IRCs) that foster global networked connectivity and asymmetric responses to conventional military supremacy. This article explores how the conceptual apparatus regarding the distinction between wartime and peacetime, as well as war zones and peace zones, which has been developed within the framework of international criminal law and humanitarian law, can contribute to military-strategic operational and capability concepts. Integration of these conceptual frameworks within strategic analysis can serve to promote the effective use of force within a full spectrum operational environment in which information, surveillance, target acquisition and reconnaissance thresholds are being raised and where deeper understandings of the social dynamic that sustains ongoing fighting within a global information environment become increasingly feasible. In this context, this article suggests that law enforcement frameworks and approaches have a high threshold of applicability if the strategic failures associated with conventional military operations are to be avoided.

Introduction

This article outlines in general terms how the environment of 21st century transnational organised crime, terrorism and unconventional conflict is being shaped by information-related capabilities (IRCs) that foster global networked connectivity and asymmetric responses to conventional military supremacy. These dynamics challenge our ability to use existing legal and strategic conceptual frameworks in order to condition and determine responses that are not only effective, but, connected to this, appropriate. In particular, both the UK Parliamentary Joint Committee on Human rights and the UK House of Commons Defence Committee have urged further clarity and consensus building as well as strategic plans for operationalising human rights law and the law of armed conflict, as the current state of affairs not only creates too much uncertainty for military personnel and human rights claimants, but is said to impede operational effectiveness.

This article suggests that although the conventional conceptual apparatus regarding the distinction between wartime and peacetime, as well as war zones and peace zones, which has been developed

within the framework of international criminal law and humanitarian law has yet to embrace fully the asymmetric strategies and unconventional means of increasing lethality fostered by global networked connectivity on the part of non-state actors; many of their fundamental principles and indicative guidelines may be integrated into aspects of our contemporary strategic thinking which seeks to describe the environment of conflict and the operations occurring within it (operating concepts), and which seeks to describe how the general shape of forces should be optimised within a full spectrum conflict environment (capability concepts).

The practical benefit of incorporating developments within legal doctrine into strategic thinking is that they may be used, firstly, to understand better the complexity and diversity of our full spectrum and globalised operational environments, and, secondly, as a way of developing and conditioning effective strategic, operational and tactical responses to the dynamics of unconventional conflicts. This approach can serve to mitigate both the problems of low-level tactical and operational engagements causing civilian harm which may result in strategic costs, and the strategic approaches to conflict that cause them to escalate and spill-over.

The 21st Century Operational Environment

According to Charles Garraway, the distinction between 'war' and 'peace' 'was never more than theoretical and in the last 50 years has broken down completely.'1 The practical significance of this distinction was noted recently by the UK Parliamentary Joint Committee on Human rights which stated that the legal line between counter-terror law enforcement operations and the waging of war by military means risks becoming blurred, and stated that urgent clarification is needed, particularly about how the international legal frameworks of human rights law and the law of armed conflict apply to the use of lethal force abroad in counterterrorism operations. This is because the former has much stricter standards on the use of force than the latter in that lethal force may only be used where absolutely necessary and operations resulting in the use of lethal force must be planned and controlled in a way that minimises the risk of loss of life.2 Additionally, the UK House of Commons Defence Committee not only raised concerns about the lack of clarity and certainty that arise out of the tension and overlap between the law of armed conflict and human rights law on the part of military personnel and civilians, but also about what it described as the increased 'judicialisation of war', whereby legal scrutiny in coroners' courts, public inquiries and cases brought under human rights law serve to impede the operational effectiveness of armed forces.3 Concerns such as these are exacerbated within operational theatres involving either brief or protracted low-intensity

fighting between states and non-state actors, or between non- state actors, both within and also across territorial boundaries.

In response to the conventional superiority of many states, non-state actors increasingly appear to be adopting asymmetric strategies and unconventional means of fighting such as concealment within civilian populations and using clandestine networks, facilitated by modern IRCs, which enable operations to be conducted with increasing global reach and with increasing lethality. Due to the complex, diffuse and fluid nature of threats within the 21st century environment, it has been increasingly difficult to characterise situations as a prerequisite to applying the appropriate legal frameworks, as well as to devise appropriate strategic operating and capability concepts as a basis for employing effective responses or lines of operations, namely those that are not purely conventional military operations in character.4 Within a single operational theatre or area of operations, there are likely to be different types of armed confrontation reaching the threshold of an armed conflict of an international and/or non- international character. Further complicating this is violence that may be associated with terrorism, uprisings, organised crime, public disorder or petty crime that does not reach the threshold of an armed conflict or which is connected with surrounding hostilities.

Broadly speaking, the 21st century operational environment may thus frequently constitute a strategic and regulatory grey area, given that it may require a mix of combat, law enforcement and humanitarian activities as there is likely to be a full spectrum or continuum of violence ranging from petty crime to armed hostilities between states or between states and organised armed groups.5 Further compounding the difficulties on how to respond effectively to grey zones of conflict and other situations of violence, unconventional operations may be protracted in nature as an outcome of asymmetric tactics whereby organised armed groups conceal themselves and lie dormant within a strategic geography that is civilianised and urbanised, but have a much larger tactical reach in that they may be globally connected to complex and diffuse networked structures that can achieve physical effects with increasing lethality, in an opportunistic fashion, at any time and in any place, and which may not be amenable to conventional military approaches.

The Global Information Environment

An important definition of the concept of an information environment is as follows: ‘the aggregate of individuals, organisations, and systems that collect, process, disseminate, or act on information’,6

as well as a group's IRCs, which are defined as 'tools, techniques, or activities using data, information, or knowledge to create effects and operationally desirable conditions within the informational, physical and cognitive dimensions of the information environment'.7 Counterinsurgency doctrine defines the 'information dimension' as the place where the physical and cognitive dimensions interact, or, in other words, the place where information is collected, processed, stored, disseminated, displayed, and protected; the physical dimension comprises targetable command and control systems in the real, tangible world such as information systems, human beings (including decision makers, leaders, and military forces), and organisations as well as the supporting infrastructure and physical networks (microwave towers, computers, smart phones) that connect them and which enable individuals and organisations to create effects, and to conduct operations across air, land, maritime, space and cyberspace domains and across national, economic, and geographical boundaries;8 the cognitive dimension is defined as existing in the minds of individuals such as those who plan, instigate or order, or those who follow them. It is the dimension where people think, perceive, visualise, influence and decide, and includes their values, ideologies, ideas, beliefs, intentions, motivations, influences, decisions and perceptions.9 Accordingly, the cognitive dimension is viewed as the most important component of the information environment because it is where effects are created and where strategic defeats can be suffered Global

Networked Connectivity

Global networked connectivity brings countries, groups and people around the world closer together. It has a stimulating effect on crises and conflicts in that it provides for the freer flow of weaponry, information and finances for groups and individuals. It allows them to have wider strategic and operational effects than in the past.11 The ability to create and control the flow of information brings with it organisational, doctrinal, strategic and tactical advantages that serve to challenge conventional legal and strategic frameworks and responses. In 1998 John Arquilla et al. suggested that network-based conflict and crime will become major phenomena in the decades ahead and that modern communications tools foster global networks which increasingly enable small and dispersed groups to communicate, coordinate and achieve effects such as armed violence outside areas that they physically control and without a precise central command or hierarchy.12 Testimony to this are the recent writings of Burke, Kilcullen and Atwan.

According to Burke, networked connectivity allows for three main types of network to operate and constantly adapt. Firstly, there are major groups or networks that are able to organise a centralised command structure in order to resource and coordinate large-scale military operations, and to

control territory as well as to incorporate subnetworks. For example, Islamic State has been able to integrate a number of Sunni militant networks into its pre- existing overarching networks. Secondly, there are smaller networked militant groups that have some degree of organised structure. Affiliates may have allegiance to and follow orders from major groups, whereas independents or factions may act autonomously of the central leadership of a major network or merely offer loose support. There is an increasing trend of affiliates and independents establishing links and loose coalitions with each other in order to coordinate their operations without directly involving the senior leadership of a major network. Thirdly, there are self-radicalised individuals or small groups that are not directly connected to major groups or smaller militant groups, but who plan and carry out acts of violent extremism, sometimes in the name or ideology of major groups, or engage in non-violent extremism online.13

According to Kilcullen, major groups such as Al-Qaeda and Islamic State are exploiting developments in IRCs, such as social media, smart phones, YouTube and Google Earth to disseminate propaganda which instigates isolated acts of violent extremism, as well as to develop new and dynamic forms of command and control over diffuse transnational networks to a greater degree. ICRs enable the widespread, but often seemingly isolated, use of guerrilla or unconventional warfare techniques – not just the 'expeditionary approach' of organising in one country, training in another, then infiltrating the target country, but forming cells within countries, evading law enforcement agencies and international travel security measures and carrying out small-scale but mass-casualty attacks.14 Similarly, Atwan notes that modern IRCs have enabled Islamic State to develop and expand a 'digital caliphate' in cyberspace, which has enabled it to network with individuals and groups around the world so as to finance and direct simultaneous and protracted acts of violence that range from small-scale attacks to large-scale military operations. Atwan suggests that part of the reason for this is that Islamic State's online social media and publications have enabled it to influence, recruit, train and operationalise a vast target audience around the world by inculcating a shared ideology and militant praxis. According to Atwan, off-the-shelf anonymity products have facilitated the development and survivability of this 'digital caliphate'.15

In this complex and cluttered information environment, it is vital to engage in social network analysis of individuals and groups within networks and to assess the information that is being disseminated in order to determine how it affects the capabilities of actors to engage in armed hostilities as opposed to criminal acts of terrorism. Strategically, it will be increasingly important, and difficult, to distinguish violent networked

insurgencies that result in effects rising to the level of an armed conflict from the networked mobilisation of civil society resulting in, or occurring within, a context of isolated attacks, potentially on a long-term basis.16 It will be a constant challenge for social network analysts to identify what we can conceive of as hierarchical or centralised forms of coordinated military organisation. They will have to be constantly on the lookout for new, dynamic and adaptive forms of organisation and ways of linking actors and groups within belligerent networks, as these are increasingly not based on formal hierarchical and networked structures of command and control involving two-way communication systems or face-to-face interaction for disseminating plans and orders. Furthermore, the cluttered information environment, mass use of social media and sophisticated 'off-the-shelf' encryption tools and techniques, especially for propaganda, makes it harder to detect those actors who are recruiting, training and planning potentially numerous attacks with long lead times, as well as to detect concerted efforts to this effect.17 In this regard, understanding the precise nature, scope, characteristics, and effects of individuals, organisations and systems that collect, process, disseminate, or act on information, is essential in order to assess whether or not there is a state of internal or transnational non-international armed conflict in existence, and, if not, to respond by using and developing law enforcement methods at the domestic and international levels. It is suggested that, the constant evolution of terrorist methods, financing using internet-based systems, quickly renders counterterrorist measures obsolete, we need to remain vigilant about understanding the social dynamic that underlies both criminal activity and warfighting, in order that we do not over extend the permissive framework due to political and military expediency. Kilcullen suggests that the advances made in cloud computing, complex systems theory, big data analysis, remote observation and crowd-sourced analytics are enabling us to map and gain insights into virtual/human support networks as well as complex patterns of violence far more easily than in the past.18 Strategically, we must use these to gain a clear understanding of the transnational information environment at any given time so as to identify the adaptive and unconventional methods of command and control, and to assess whether a group's organisational, fighting and logistical abilities mean that it has the ability to carry out sustained and concerted military operations in such a way that exceeds the capacity of law enforcement agencies to respond.19

The Virtual Theatre of Conflict

The global information environment also undermines our spatial or geographical conception of a war zone.20 In other words, it is increasingly difficult for policy makers as well as military strategists and lawyers to ensure that 'war zones' or areas of operations, and thus law of war permissions, are

confined to areas where military forces are physically located and directly engaged with enemy forces. In turn, this makes it a challenge to resist spill- over into 'peace zones' where the intensity of violence generally does not reach the threshold of a non-international armed conflict, but which nevertheless contains concealed and supportive elements of a transnational network that are virtually connected to the zone(s) where armed conflicts are physically located, and where physical effects are produced by virtue of a range of indirect support roles that are performed remotely using IRCs from outside the territorial boundaries or strategic geography within which conflict physically occurs. Support functions within a 'virtual theatre' may include command and control, logistical support, the dissemination of intelligence of a military nature, the recruitment and training of individuals, and even the provision financial support.

Approaching the Complexity of the Information Environment

Increasingly, traditional conceptual frameworks that are framed around single threats or simple binary distinctions may not be regarded as being fit for a complex information environment which comprises diverse actors within diffuse networks that are competing for influence and control, and which are able to use IRCs to adapt their various activities with greater ease, frequency, reach and lethality.21 Accordingly, concepts and capabilities should be developed and employed so that adequate assessments can be formed as to whether the command and control, organisational, fighting, information and logistical abilities of a group or network mean that it has the ability to carry out protracted military operations in such a way that actually exceeds the capacity of law enforcement agencies to respond.22 If not, then it is questionable as to whether we can legally define the situation(s) as constituting an armed conflict and apply conventional military approaches within the framework of the law of armed conflict without this ultimately being strategically counter-productive. Indeed, it has been argued that conventional military approaches adopted since the beginning of the 21st Century have turned out to be 'a strategic failure' and 'represent nothing less than the collapse of Western counterterrorism strategy' as they have cost us our 'strategic freedom of action and eroded the legitimacy of a cause that, at the outset, enjoyed huge global support' and have created 'a stronger and more motivated, more dangerous enemy'.23 Although forming a definitive snapshot of the operational environment as a basis for predicting and forming the necessary responses may not be possible in such a complex information environment that is in a constant state of flux,24 it is still necessary to optimise forces for this environment by developing an astute situational understanding in any given situation.

Accordingly, for legal and strategic responses to be effective and appropriate in this complex environment, their conceptual frameworks should complement each other and be used to form assessments that constantly remain abreast of how actors are using IRCs to adapt asymmetric strategies and unconventional methods in order to produce effects within the physical domain. This can be done through continuing to develop and employ information, target acquisition and reconnaissance capabilities (ISTAR) that can improve the threshold and accuracy with which threats can be detected by, firstly, ensuring that adequate information gathering capabilities exist and that information can be integrated, processed, and disseminated at strategic, operational and tactical levels of command;25 and, secondly, ensuring that there are personnel at all levels who have adequate cultural and linguistic understanding so that the social dynamic that sustains fighting can be understood and so that the cognitive dimension, comprising individual and group intentions and motivations, can be understood, and to tailor force size, structure and capabilities to respond quickly to operational environments that are rapidly changing and to tailor rules and effects that are appropriate to the circumstances.26 Even though global connectivity renders it increasingly difficult to create legal, strategic and operational boundaries between 'peace zones' and 'war zones', this article suggests that we should use and develop legal frameworks on conflict classification to ensure that the physical domain of the paradigm of hostilities does not track and extend out into the peripheries of the virtual domain, especially because, as noted by Kilcullen, this can draw in populations and forces anywhere on the planet that have no geographical connection to the conflict, in the sense of being directly involved in conduct or support.27

The Strategic Importance of the Legal Characterisation of Conflict

Legal characterisations and conceptual frameworks applicable to a situation or state of affairs are of practical relevance to strategic thinking and analysis as they establish the legal frameworks within which military operations, and, increasingly, information operations, take place. Their integration into strategic thinking and analysis can serve to avoid strategic failures and defeats, such as those where relatively calm situations are escalated and become far more dangerous; where targeted killings or tactical overreactions could be based on manipulation or intelligence failures, for example, being used by one faction against another as part of a vendetta or dispute;28 or where targeters make 'positive identification errors' because they erroneously presume civilian behaviour to be hostile or suspicious or because they have differing interpretations of what it means directly to participate in hostilities or be a member of an organised armed group – issues which are beyond the scope of this enquiry.29

The law of armed conflict is similar to human rights law in that individuals can be targeted using lethal force for such time as they pose a direct and immediate lethal threat, e.g. in self-defence. Where they differ is that within a situation of armed conflict, individuals can also be targeted at any time and in any place where they have the status of a member of an organised armed group exercising a continuous combat function, i.e. they lose their civilian status and need not represent a direct and immediate lethal threat at the time of attack. In general terms, human rights law does not tolerate such intentional, premeditated and deliberate use of lethal force unless absolutely necessary. Furthermore, the transition to the framework of hostilities opens the way to law of war permissions on the use of force that are much more permissive than human rights standards when it comes to taking precautions in attack and scrutinising incidental loss of life, injury and damage. Determining the overall legal framework is both a major protection issue as well as a vital strategic consideration. Where attacks are perceived as indiscriminate or as causing excessive incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, then these tactical or operational issues may have strategic costs which undermine the effectiveness of the use of conventional military force. The legal frameworks of law enforcement and hostilities serve to condition the nature and extent of force that is permissible, and may therefore act as a safeguard against inappropriate types and degrees of force which military doctrine recognises as having the potential to be counter-productive, for example, by serving to escalate crises or conflicts which render the return to peace and public order unnecessarily difficult. Connected to this, the application of one legal framework instead of another serves to establish common standards and expectations in the context of information operations within a complex global information environment. In what is often described as ‘lawfare’, the resort to legal norms may be used by governments in order to clarify an justify, for example, why the legal framework of armed conflict, rather than the human rights based framework of law enforcement, applies to the use of lethal force in order to manage public opinion in response to the effects of operations that occur at the tactical level of war, especially where they can be manipulated by one side of an asymmetric conflict in order to contribute to or cause adverse strategic consequences.

As the use of conventional military force in ‘grey area’ operational theatres that are increasingly civilianised and urbanised, such as counter-terrorism and counter-insurgency operations, has the potential to create civilian harm that may easily be perceived as excessive, it is suggested that our legal and strategic conceptual frameworks should be used together in order to prevent the framework of hostilities from ‘coming down’ from its high threshold of applicability into situations of social crisis or public emergency, as this could serve unduly to legitimise targeted killings and the use

of high-intensity means and methods of conventional military force across a range of low- intensity hostilities.

Situational Classification Criteria Developed within International Criminal Law

The indicative guidelines developed within international criminal law for determining the existence of a non-international armed conflict will now be discussed, given that they constitute useful tools for forming appropriate and effective strategic pictures and responses, and, in particular, for assessing whether or not conventional military lines of operations are likely to be appropriate in any given area of operations. It is suggested that where the criteria given below have not been established, then human rights based law enforcement lines of operations should be employed.30

The Intensity Criterion

Pertinent to the issue of identifying where the framework of law enforcement cannot be expected to operate are whether the hostilities are of a sufficient intensity to qualify as an armed conflict.31 Another way of putting this is whether the hostilities can be considered sufficiently serious and whether there has been an increase in and a spread of armed clashes over territory and over a period of time.32 In this regard account ought to be taken of the casualty levels33 and the extent of the destruction34 caused by the fighting as well as the effect of hostilities on civilians, for example, by forcing them to flee from combat zones, and whether civilians and/or civilian objects have been subject to direct or indiscriminate attacks.35

An assessment should be made as to whether it has been necessary to increase the size of government armed forces in response to the intensity of violence, as well whether there has been significant mobilisation and distribution of weapons among both parties to the conflict.36 Indicators in this regard include whether it has been necessary to increase troop and unit deployment numbers, the formation and change of front lines between belligerent parties,37 and whether it is necessary to use high intensity 'weapons of war' such as 'heavy weapons and other military equipment, such as tanks and other heavy vehicles'.38 Also relevant to the issue of mobilisation of forces and matériel is whether it has been necessary to employ military tactics and formations, such as the mass deployment of forces to a crisis area, the closure of roads and the blocking and encirclement of conurbations and the use of mortar or artillery fire against them.39 Another key factor that is relevant to the intensity criterion is whether international organisations such as the UN Security Council have become involved over concerns about the situation presenting a threat to

domestic, regional and international stability, and whether any resolutions have been passed in this regard.40

An account of the intensity or seriousness of hostilities may also take place at a more systematic level in order to build up a common operational picture.41 Strategic analysis should consider the policy decisions, on a whole nation basis and across military hierarchies, that lie behind the way that organs of the State, such as the police and military, use force against armed groups at various levels. The rationale of this systemic approach is that such considerations may indicate that it has been necessary to make a tactical and operational shift away from the framework of law enforcement to that of armed conflict because the former has become unfeasible or too dangerous in the circumstances.42 In this regard, account may be taken of the nature of the orders and instructions given to forces engaging in clashes with organised armed groups, and whether forces are limited to using force that is 'no more than absolutely necessary and which is strictly proportionate to certain objectives' or whether forces have been permitted to use lethal force under broader and more permissive rules of engagement.43 This is particularly important in grey area situations where there has been no formal declaration of war or state of emergency. In such instances, an analysis of orders and instructions running down a chain of command may be probative of tactical and operational assessments that the intensity and seriousness of the violence is such that the law enforcement model is too restrictive of the use of force, and that the framework of armed combat has become necessary to restore control, public order and security. However, in an environment that is diverse, given the diversity of actors involved, and ambiguous, given the range of lethal capabilities at the disposal of non-state actors, we may also, where feasible, look to the devolved situational awareness and decision capabilities made at lower levels of military hierarchies. This is because they may be optimised at the tactical and small-unit levels so that forces can effectively identify and respond to threats in fast-changing and chaotic situations.

In this way, tactical and operational decisions are part of a number of factors that may go towards a broad assessment of how the underlying state of affairs should be qualified and responded to and how strategic assessments need to be open to operational and tactical assessments. The existence of these factors suggests that the law enforcement paradigm consisting of individualised threat assessments and law enforcement techniques may no longer be practicable, and so we must introduce the framework of hostilities out of military necessity.

The challenge for making assessments in this area is that states will respond to exceptional circumstances, such as terrorism cases, in a range of ways. Some states may respond through their ordinary criminal procedures, whilst others have established exceptional procedures and rules on the use of force, detention, evidence and trial procedure that are enforced through specialised or even military courts.44 In order to assess whether or not this law enforcement paradigm is practicable, we need to assess whether the police, prosecutorial and judicial institutions and their general or specialised law enforcement tools can operate effectively in the face of the exceptional circumstances within the overall security environment. To this effect, the United Nations Counterterrorism Committee has provided technical guidance to states which would suggest that exceptional criminal procedures and special investigative tools can be employed across a broad spectrum of serious criminality, including serious organised crime and terrorism.

Factors that may be taken into account in assessing whether law enforcement mechanisms have the systemic capabilities to respond to exceptional challenges include whether the police, prosecution and judicial services have the capability to guide, instruct and supervise the work of the investigatory agencies and whether the police/military investigators themselves can operate within in the security environment: for example, there may be 'no go' areas for the police/military, precluding them from gathering evidence, carrying out crime scene investigations, interviewing victims and witnesses; from controlling the use of special investigative techniques by investigative and prosecutorial agencies; from handling complex cases involving conspiracy, charity law, finance, and human rights as well as being able to map out complex networks and typologies of incitement and recruitment; from handling and securing forensic, technological and financial aspects of investigation and prosecution; from cooperating internationally both formally and informally; from executing correctly mutual legal assistance and extradition requests; from supervising the use of special investigative techniques by the investigative agencies; from handling intelligence collected by the different investigative agencies and converting it into admissible evidence when appropriate; from handling evidence collected by different States; from accessing special training or educational programmes concerning criminal networks and criminal financing; from accessing intelligence and intelligence techniques such as covert surveillance and infiltration; from handling anti-terrorist financing measures (for example, freezing, confiscation); from responding to transnational crimes that can support or facilitate terrorist activity; from handling witness protection for victims, witnesses and collaborators before during and after statements and testimony are given, bearing in mind that they will be subject to intimidation and death threats; from handling investigative and pre-trial detention of suspects, potentially in large numbers, in accordance with procedures established in law, without

having to resort to prolonged or indefinite periods of detention due to security risks or political exigencies and without causing the security situation to escalate further in intensity; from running special courts and court procedures, without necessarily resorting to military courts, and ensuring that there are fair, and, where possible, public trials by independent and impartial tribunals (that is, investigating and judicial authorities that are, and are seen to be, operationally independent of the military chain of command).45

The Organizational Criterion

The second factor to consider in assessing whether a strategic decision should be made to operate within the framework of the law of armed conflict is whether a network has the requisite level of organisation. The more organised a network is, the greater the threat it represents, and therefore the greater the challenge it will be for the 'normal' framework of law- enforcement to respond. This organisational prerequisite is an important factor to consider in determining whether standard means and methods of law enforcement are inadequate, and military means and methods are therefore needed to re-impose public order, or, in other words, whether an armed group forms part of a network that is so well organised that it exceeds the capacity of law-enforcement mechanisms to respond. Zemach frames this in a slightly more nuanced fashion by describing situations that exceed the capacity of the law enforcement model as those which generally preclude the possibility for individualised threat assessments and law enforcement techniques.46

In these ways, the organisational criterion is related to the intensity criterion, but it is also an important element in its own right in that the law of armed conflict framework can only apply in a pragmatic and functional sense where a group has the requisite organisational structure and capabilities. Thus, in general terms, to constitute an organised armed group, there needs to be 'some hierarchical structure' and furthermore the 'leadership requires the capacity to exert authority over its members'.47 Thus, for the law of armed conflict to apply, basic organisational features need to be in place so that it can. In this regard, '[s]ome degree of organisation by the parties will suffice to establish the existence of an armed conflict' and that '[t]he leadership of the group must, as a minimum, have the ability to exercise some control over its members'.48 Without this functional pre- requisite in place, it may be suggested that 'those who regard its actions as mere acts of anarchy or brigandage are right',49 which in turn suggests that a law enforcement model is the appropriate and necessary legal and policy framework with which to regulate the use of force in response to 'irregular, anarchic armed groups with no responsible command'.50

In general terms, it may be suggested that 'irregular, anarchic armed groups with no responsible command' may not exceed or undermine the capacity of an intelligence-led and evidence-based law enforcement model to respond, as they are not sufficiently organised to confront police and military forces with military means. However, they do not need to be 'as organised as the armed forces of a State' in order to satisfy the organisational criterion and they do not need to control territory.51 Five indicative and interrelated criteria of what constitutes a sufficient degree of organisation on the part of a non-state group for it to exceed the capacity for law enforcement mechanisms are now outlined.52 Firstly, there must be some form of command structure in place. This may be evidenced by the existence of what can be regarded as a 'general staff' or a 'high command' which can issue political statements and communiqués as well as organise personnel, logistics and weapons, such as by appointing personnel to specific roles or tasks, giving orders and authorising military operations.53 This command structure must enable a 'high command' to receive reports from all operational units within the chain of command and to establish and disseminate internal regulations that set out the hierarchical organisation and structure of the armed group in terms of roles and duties at each level of the chain of command.54 Secondly, for a group to qualify as being 'organised', it must have the ability to carry out military operations in an organised fashion and control territory. Factors to consider in this regard are whether the group has the ability to establish a 'unified military strategy' so as to be able to conduct large scale or protracted military operations, whether it has 'the capacity to control territory' (rather than actually controlling it), and whether 'there is territorial division into zones of responsibility'. Furthermore, there must be some evidence that commanders and operational units can 'co-ordinate their actions' and effectively disseminate 'written and oral orders and decisions'.55 Thirdly, an organised armed group is one which has a sufficient level of logistical and organisational capabilities. For example, an assessment is to be made of a group's ability to recruit new members and to provide them with military training and to control and organise the supply of weapons and uniforms as well as its ability to link and co-ordinate all levels of the chain of command through a communications system.56 Fourthly, an armed group must also be sufficiently organised so as to ensure a level of discipline. Factors relevant in this respect include whether there is a system of internal regulations and disciplinary rules in place, as well as mechanisms such as proper training and supervision to ensure that they are disseminated to members of the organised armed group.57 Fifthly, we must consider whether the group or network has the ability to "speak with one voice" in the course of political negotiations.58 In this regard, account may be taken of the group's capacity 'to act on behalf of its members in political negotiations with representatives of international organisations and foreign countries' as well as its ability to negotiate and conclude agreements such as cease fire or peace accords'.59 The existence

of these organisational features may indicate that standard law enforcement means and techniques may not be able to remove or reduce the threat from an organised armed group.

War and Peace in the Information Environment: An Application of the Intensity and Organisational Guidelines to Networked Conflicts

This part of the discussion will now tentatively apply these indicative guidelines to operations that have occurred within the information environment in order to provide worked examples of how they can influence strategic assessments on whether to approach situations within the human rights based framework of law enforcement or within the framework of the law of armed conflict.

Command and Control

Increasingly, we see that IRCs, such as cell phones and social media, are used to plan and order attacks. In view of the indicative guidelines above, we need to examine whether the physical, information or cognitive dimensions present elements of a basic command structure with a recognised leader, structure and hierarchy, and internal regulations that establish a chain of command and disciplinary measures. A network analysis of the information environment may help us to understand the organisational dynamics and thus the nature of the threat that we face. Furthermore, it may help us to understand where the leadership resides and how it is distributed among members within the network.60 For example, Kilcullen notes that from mid- 2015, Islamic State wilayat networks had been established in Libya, Algeria, Tunisia, Yemen and Egypt. Rather than being viewed as mere guerrilla or terrorist groups, these were seen as formal territorial, legal and political entities with direct connections to a centralised caliphate organisation and a central figure by the name of Abu Bakr al-Baghdadi who was able to set out the overall aims and objectives of the group together with his two deputies, Abu Muslim al-Turkmani and Abu Ali al-Anbari, and a variety of advisory councils and departments such as the military council and the security and intelligence council. Through this effective chain of command over large fighting and auxiliary forces, Islamic State conducted operations within a set of defined strategic guidelines and collaborated with networks in neighbouring regions which were able to carry out larger, widespread and coordinated attacks in Syria, Libya and Iraq. Some of these were coordinated large scale attacks, whilst others were smaller self-radicalised attacks. Islamic State executive leadership began to establish territorial control comprising a network of cities linked by narrow strips of territory in Syria and Iraq and to carry out state like functions, such as running courts, taxation, public services as well as intelligence

and security services. Islamic State has also been able to recruit and receive vast numbers of foreign fighters travelling to Iraq, Syria, Libya, Yemen and Somalia. In areas such as these, Islamic State represents more of a conventional military threat to other non-state actors as well as other states rather than a terrorist group per se. This is especially so that it can finance its operations from a diverse range of revenue streams such as control over oil fields, trafficking in weapons, drugs and artefacts, kidnapping and robberies. However, although major groups such as Islamic State and Al-Qaeda may be able to launch conventional attacks in the Middle East, we must closely examine their links with peripheral actors and networks in other regions in the Middle East, Europe, Asia and USA as well as the roles and capabilities these peripheral actors are performing, in order to assess whether the overarching network has the organisational resources and capabilities to launch widespread and coordinated attacks in these regions.61

Accordingly, at the strategic and operational levels, where a group's IRCs allow for an identifiable leadership to plan, order and coordinate large-scale attacks, even if this is done remotely and by dispersed groups outside their physical control, then there is the potential for this to reach the level of transnational non-international armed conflict. However, it is important for there to be some control and effect over an insurgent network that exists in the physical and cognitive domains. It is suggested that there does not have to be complete control over these domains at all times, as this is not realistic in an information environment with a high degree of surveillance that compels groups to avoid detection by adopting diffuse structures.62 Accordingly, there may be no clear organisational structure that mirrors a conventional chain of command involving a core leadership, guerrillas, cadres, auxiliaries and underground cells. Thus, rather than a hierarchical leadership structure, the organisational structure may be diffusely networked within a complex and cluttered information environment involving a range of actors or entities that provide basic support functions and this network will be constantly learning and adapting.63

In a networked organisation it is important to understand the roles that actors play in a network and the links that exist between them for financing, as well as providing tactical and operational support, to produce effects that are adverse to the military operations or military capacity of a party to an armed conflict or, alternatively, that inflict death, injury or destruction on persons or objects protected against direct attack. What we are looking for primarily are 'critical actors' or central points of communication or influence that have an influence or measurable impact on a network that is capable of carrying out military operations in the physical domain.64 Critical actors have a great influence over what flows through the network and are able, directly or indirectly, to influence

other actors within that network.65 In particular, they will have a measurable impact upon what we may describe as underground ‘guerrilla units’ or ‘cells’ which are able to carry out small-unit tactical operations or which can mass or coordinate for larger operations, for example, directly recruiting and providing some tactical support or indirectly providing general guidance and support, thus enabling a pattern of individuals to self-recruit and operationalise in the name of the cause or strategy, for example, what may be described as a digital levée en masse or mass uprising.66 The information environment may indicate a highly centralised network that is dominated by one or more centralised actors. However, if these actors are removed or damaged, then the network may fragment into unconnected subnetworks.67 Where such fragmentation or disaggregation occurs then a decentralised network may result. A characteristic of this is that there is now no single point of failure, as operational and tactical decisions may be made by different actors within the network rather than by a central or critical actor. A major network may fragment into numerous subnetworks that have numerous connections to the operational environment, but not necessarily with each other. Here, subnetworks may have direct multiple connections with each other; they may have only very loose and indirect links with a few central actors and other subnetworks; they may now be completely isolated and freestanding.68

Under such circumstances, it is important for us to gauge network density, which is a general indicator of how connected individuals are in a network – the more links that actors have to other actors within a network, the greater the density.69 Decentralised networks may have low network density and be complex to map. In other words, unlike a hierarchical network, low network density means that such networks are not acting as a unified force, but rather as a disaggregated and atomised force.70 Under such circumstances, it is unlikely that a central actor will be able to enforce discipline, ensure that orders are carried out and that there is compliance with internal rules or discipline. However, a central actor may still be able to issue general, albeit one-directional, ideological, operational and tactical guidelines to their target audience. They may still control what flows through the network and have great influence over peripheral actors without having direct links to them or direct influence over them.71 Kilcullen notes the contemporary phenomenon of self-recruited individuals or groups acting upon general directions, propaganda, tactics and techniques, usually disseminated openly on the internet by ‘symbolic’ or charismatic figures without their having to give any direct communication, support or coordination. Kilcullen terms this form of remote radicalisation and operationalisation as ‘leaderless resistance’. More specifically, the individuals and groups who carry out violence ranging from small acts of violent extremism to large-scale military operations may be extremely peripheral in that they have no direct ties to central

figures or networks and are operating in a clandestine fashion in foreign countries. Central figures do not have to establish a formal hierarchical structure or chain of command based upon two-way communication systems in order to disseminate secret plans and orders, but merely make public statements and general commands on YouTube or social media. These then become linked via social media platforms to other actors who issue detailed operational and tactical guidance enabling individuals or small groups to act autonomously and on their own initiative. For instance, Anwar Al-Aulaqi was designated as a 'Specially Designated Global Terrorist' because he was said to have provided financial, material or technological support for actors of terrorism that included recruiting, influencing and training persons to fight, such as Nidal Hassan, who fatally shot thirteen people and injured more than thirty others in the Fort Hood mass shooting on 5 November 2009, and Umar Farouk Abdulmutallab, who is popularly referred to as the 'Underwear Bomber'. Al-Aulaqi is also said to have inspired the London 7/7 attacks as well as plots in Toronto in 2006 and Fort Dix in 2007 through his sermons available on the internet and on DVD.72

This state of affairs necessitates rigorous social network analysis of the information environment in order to understand the organisational dynamics of a network and its leadership. We need to identify the nature and scope of leadership and how it is distributed throughout a network. It may be that members have a high degree of autonomy which enables the network to avoid detection and increase its operational capabilities.73 It is suggested that even though central actors may be unable directly to enforce discipline, to ensure that orders are carried out and that there is compliance with humanitarian law, this is not necessarily detrimental to a networked group being sufficiently organised for the purposes of applying the paradigm of hostilities. Under such conditions, we should be careful to ensure that there is reliable intelligence that indicates a pattern of individuals or cells indirectly responding to and operating in a manner that is consistent with the general guidance issued by central actors (for example, by following instructional videos or audio files or training manuals and by publicly professing a commitment to the cause). Furthermore, in the absence of a hierarchical structure made up of a direct chain of command, we would need sufficient intelligence to demonstrate a pattern indicative of a unified fighting force, namely, that remote leadership is inculcating similar ideological, tactical and operational decisions and effects across a decentralised network. Where this is not the case, then this would indicate that the network does not constitute a sufficiently unified or organised fighting force capable of mounting adverse military operations.74

Ability to Mount Protracted Operations

We need to examine the information environment in order to assess whether a group's information-related capabilities and network dynamics enable it to conduct protracted or sustained and concerted military operations, such as manoeuvring fighters and carrying out coordinated hit and run operations. We need to examine whether IRCs are being used to coordinate military grade logistics, such as such as supplying weaponry and equipment, financing, providing military training and recruiting new members. There should be evidence in the information environment that a network has some unity and the ability to speak with one voice. In our modern information environment, IRCs, such as cell phones, text messaging, voice over internet protocol, GPS devices, Google Earth and the internet, are being used to organise and coordinate actors within networks. Urban populations within developing countries are now highly connected and networked, expanding their reach, influence and support.75 According to Kilcullen, the same connectivity that enables licit trade also enables people to self-organise in 'dark networks' where illicit trade, trafficking, piracy and terrorism flow.76 Furthermore, 'dark networks' may be used to enable violence across a spectrum ranging from criminal activity through to transnational terrorism and transnational non-international armed conflict.77 Accordingly, we need to be careful in examining IRCs in order to assess whether they are being used to conduct coordinated and large scale military attacks, even by what may appear to be a decentralised and fragmented organisation in the physical domain.78 For example, Kilcullen notes that in the 2011 Libyan uprising, groups used social media platforms and networks through improvised satellite phones and internet uplinks for remote and decentralised command and control. The command system was distributed through multiple networks and remote platforms and was used to play a practical coordination and logistics function for self-organising corps of volunteers and non-state armed groups, for example, by developing a narrative or common cause, distributing military intelligence, tactical and operational guidance as well as sending out requests for assistance. According to Kilcullen, this allowed 'a diverse movement of small groups, spread across several coastal cities to act in a unified manner against the regime, making this a true case of networked-enabled insurgency [with] supporters of the uprising from all over the world'. Effectively, Libya in 2011 was a novel example of a mass networked mobilisation emerging in cyberspace that had direct physical effects rising to the basic intensity threshold of an armed conflict.79 Thus, where a group's IRCs allow for the detailed planning, organisation and coordination of attacks as part of large-scale military operations, then a group's network may be regarded as sufficiently organised for the purposes of applying the paradigm of hostilities.

Returning to the idea of network density, where the information environment reveals a high network density among a range of actors and entities, this would indicate that a group has the networked capabilities to conduct widespread, coordinated and protracted military operations. This means that they may be sufficiently organised to constitute a dangerous military threat and thus subject to the framework of hostilities.80 Accordingly, this involves an assessment of a network's ability to share information in near real time, anonymously and securely, and then to act on it in a coordinated fashion.81 To this end, we would need intelligence regarding direct and/or indirect links between auxiliary cells and guerrilla cells as well as the ways in which a group is using IRCs to recruit, train and motivate followers, organise the logistics of weaponry and people as well as the financing of military operations.82 For example, we would need evidence that there are auxiliary cells that perform logistics operations such as maintaining safe houses, moving weapons, intelligence gathering, propaganda, recruitment and communications support.83 Auxiliaries may also include economic support systems that directly fund military and political operations, such as fund raising, unlawful appropriation, illicit trade and trafficking, banking and finance operations and laundering through businesses.84 We would need intelligence demonstrating that leadership and/or auxiliaries have direct and/or indirect ties to guerrilla units or cells that can conduct coordinated and protracted small-unit tactical military operations or which can mass for larger protracted military operations.85 For instance, the Mumbai terror attacks of 2008 saw a leadership cell operate from a safe house in Pakistan by giving intelligence, directions, instructions and warnings to small attack units on the ground in India by using Skype, SMS text messages and mobile phone calls. Although this caught Indian security forces by surprise and enabled attack forces to take diversionary countermeasures for a short period, ultimately it did not exceed the capacity of India's counterterrorism force to contain the attackers eventually; this small-unit tactical operation was directed at civilians rather than a large military operation or a coordinated series of assaults against police or military forces.86 This can be contrasted with the unrest in Kingston in 2010 when Jamaican authorities attempted to enforce a US extradition request of Christopher Coke – the head of an international crime syndicate named 'the Shower Posse' which controlled the Tivoli Gardens area of Kingston and had previously attacked police stations. It exceeded the capacity of civilian law enforcement to respond as it required a full scale military effort lasting around a week and involving over a thousand police and soldiers engaged in house-to-house fighting with large numbers of casualties to gain control over Tivoli Gardens.87 Nevertheless, the situation was declared a state of emergency and, overall, it was treated as a law enforcement operation to arrest and extradite, rather than kill, Christopher Coke. He eventually pleaded guilty to racketeering and drug-related charges in a New York Federal Court.

A decrease in network density indicates that a group is becoming fragmented and isolated and that its organisational ability is reduced. As a network's capability to act as a unified fighting force is diminished, it becomes less of a military threat and more amenable to law enforcement methods. Furthermore, disaggregated and atomised groups are more difficult to detect and disrupt, and so may require a more intelligence-led and individualised social network assessment in order to understand their capabilities and the threat that they pose over time.88 Another complicating feature of social network analysis is that a network may be diffusely made up of a range of criminal, guerrilla and auxiliary entities as well individuals acting alone without any direct connections to any other individuals or groups within the network.89 Some of these entities may not be aware that they are playing indirect support roles within a network that contains belligerent elements. Changes to network density and belligerent functions across a network should be continuously monitored and mapped out over time allowing states to develop and change their tactics so that they are more in line with law enforcement operations as a group's IRCs become reduced, its network becomes more fragmented and its military capabilities diminished.90 For example, Kilcullen notes that at the time of 9/11, Al-Qaeda had an organised and hierarchical network of commanders, committees, camps, groups and support networks. This high network density exposed it to attack, and so it quickly fragmented and developed forms of 'leaderless resistance' using IRCs to influence target audiences to support its efforts and to mount attacks. This process of disaggregation led to a proliferation of smaller attacks from isolated groups, factions and affiliates. However, as seen with Islamic State, its major networks have been able to disaggregate under aerial bombardment and move into safe zones, only to reform and expand military capabilities in and across new areas.91

However, even where network density is low and its elements are atomised, in our modern information environment the network may still be able to carry out what amounts to tacitly coordinated military operations where central or critical actors issue general and one-way operational and tactical guidelines that are operationalised and acted upon by isolated but free-standing and autonomous individuals, auxiliaries, guerrilla units or underground cells. Under such circumstances isolated subnetworks may have their own leadership, fighters and auxiliary forces, enabling them to mount widespread attacks.92 Kilcullen notes that groups such as Al-Qaeda and Islamic State are increasingly disseminating their tactics and techniques via online magazines, such as 'Inspire' and 'Dabiq' which enable individuals and groups to operationalise and mount attacks without any direct contact or formal membership of a terrorist organisation.93 Under such circumstances, it may be sufficient for individuals or cells to act in a manner that is consistent with general guidance without the need for further centralised operational and tactical support and

coordination as long as there is intelligence revealing a pattern to this effect. It may be the case that there is a small networked group with actors on the periphery with very few, if any, links to this central core. This may be the case where there is a group within one country and a number of 'lone wolf' actors on the periphery in other countries. This would tend to indicate that the organisation has a low network density and has a weak connection to its centre. In order to understand the nature of the threat they present, it is important to examine the nature and scope of their connection to a central network as well as networks outside the theatre of operations and in order to assess whether they contribute to the efficiency, cohesion and operational capability of a network.94 In this regard it is important to make a cautionary note in that global connectivity has increased the threat of 'home-grown terrorists', whereby individuals and groups become remotely radicalised and organised online through propaganda on social networks and social media, very often with little or no face-to-face contact with foreign terrorist groups, and gain basic training on tactics and weaponry to carry out small scale attacks. Many, if not most, of these remotely organised plots and attacks do not represent a strategic or military threat to their countries as they are disaggregated and atomised individuals or cells which are amenable to counterterrorism operations by law enforcement agencies, that is unless they begin to become more widespread, coordinated and protracted, which is generally not the case at present due to Western and European domestic counterterrorism efforts. For example, Kilcullen suggests that in some instances, attacks may not be viewed as a single terrorist incident, but rather as one part of a sustained campaign of guerrilla warfare. This might be said of the Paris attacks of January and November 2015. However, Kilcullen argues that although they represent an escalation in terms of the guerrilla means and methods of warfare, and although there is evidence linking the Paris attacks to a transnational support network as well as attacks in other countries, it is suggested that these are not sufficiently widespread, networked or intense enough to rise to the level of a transnational armed conflict. Furthermore, even though individuals or groups acting in the name of Islamic State increasingly claim responsibility for attacks, there is often little or no evidence to suggest that they actually planned, resourced and coordinated attacks. Accordingly, it is suggested that many instances of what Kilcullen describes as 'leaderless resistance', 'guerrilla terrorism' and 'remote radicalisation' are to be situated within the framework of law enforcement. Just because actors or small networks can remotely radicalise and launch attacks in the belief that they are part of a bigger network does not mean that they are actually part of a network that can launch widespread and coordinated operations in the face of a system of law enforcement that can effectively respond to this complex threat, whilst at the same time upholding human rights and civil liberties. This is an important issue given that we will be dealing with these types of threat over a long period of time and so we must

resist attempts to aggregate atomised attacks and plots into a persistent and long-term armed conflict.95 Similarly Atwan and Burke suggest that although Islamic State has developed a global jihadist network in cyberspace, this may not translate into a network that has military capabilities or the ability to create effects in the physical dimension. Instead, it may be regarded as a set of subnetworks that create effects, most of which do not rise above the level of what we could describe as non-violent or even violent extremism, which expresses similar if not shared ideas and statements. Individuals may republish propaganda on social media, condone militant activities in comments on or profess allegiance or sympathy on YouTube.96

As the notion of a 'conflict zone' is unclear within both legal and strategic frameworks, and thus the geographical scope of application is unclear, it is suggested that social network analysis is important to try and confine 'war zones' to physically confined areas where fighting forces are engaged directly, and to resist spill-over into 'peace zones', where the intensity of violence does not reach the intensity suggested above in the indicative guidelines, but that may contain concealed and supportive elements of a unified virtual network. However, even though global connectivity renders it increasingly difficult to create legal, strategic and operational boundaries between such zones, we should constantly attempt to ensure that the physical domain of the paradigm of hostilities does not track and extend out into the peripheries of the virtual domain, as this creates the risk that the conduct of hostilities paradigm can spill over and prevail outside combat zones. In this sense 'virtual theatres' can serve to undermine the spatial conception of a war zone.97 This renders the requirement that a group controls territory or has the ability to do so even more critical in setting out spatial bounds of the paradigm of hostilities, and we must closely scrutinise the ability of central actors to maintain direct and continuous connectivity with coordinated fighting units over vast virtual networks which create effects in the physical domain of hostilities. Where actors are 'virtually' in a remote 'war zone', but physically present in a 'peace zone' that is geographically disconnected from actual hostilities, then we should consider whether law enforcement methods and international cooperation are sufficient to respond to the 'virtual threat' that they present in their peace zone, and, if not, then ensure that any targeted killing is as attenuated as possible so as to be in accordance with what is justifiable on the basis of law of war targeting principles and self-defence. However, outside the context of an international armed conflict, the city, region or country where they are residing should not be treated as a war zone subject to the paradigm of hostilities. Where individuals and underground cells are self-recruited and freestanding, it will be extremely difficult to demonstrate that a 'critical actor' has caused their actions and that they are actually part of networked organisation that can adversely affect the military operations or military capacity of a

party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack. Central networks may claim responsibility for attacks, but this may often be mere pretence. It will also be a challenge to identify the ability of a network to 'speak with one voice' and for central actors to ensure uniform disengagement from a digital levée en masse. Whilst certain parts of a network may be disrupted or neutralised, other parts may continue fighting or lie dormant and opportunistically launch an attack where the opportunity arises. This suggests that such an organisation will be more amendable to law enforcement methods.98

Assessing Belligerent Nexus in the Information Environment

In an unconventional environment it is a major challenge to establish a nexus between an individual and any surrounding hostilities, either on the basis of their direct participation in hostilities or their membership of an organised armed group, in order to categorise them as a lethal threat. Where an individual does not constitute a direct and immediate lethal threat, recourse will have to be made to the information and cognitive dimensions in order to ascertain their intentions and motivations, as, more often than not, this will be the decisive issue when it comes to targeting on the basis of status and ensuring that it is done legitimately and lawfully. This requires us to understand the information environment in order to build up a picture not only of an armed group but also of the population in which it resides. We must engage in social network analysis to build up an intelligence picture of the 'social dynamic that sustains ongoing fighting', how individual actors interact with one another and how networks are being used for warfighting. In most civilianised operational environments, this will require an individual-level analysis, and the IRCs that states have at their disposal render this practical and feasible in many situations. Not only that, the use of IRCs can also help us to distinguish between those who foresee or intend adversely to affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack and take some practical contribution to this end from those who merely provide indirect support without foresight or awareness, or those who merely sympathise with the cause. From the information environment, we may be able to glean intelligence of an individual's subjective state of mind through statements, pictures, photographs, media files, private communications in cyberspace, or to make an objective assessment on the basis of their behaviour or tacit knowledge.99 Although it is beyond the scope of this discussion, one of the implications of violence within our information environment is that whilst there may be many purportedly justifiable invasions into our privacy within the information domain and public physical domain, the very existence of the global information environment should help states understand the

nature, scope and capabilities of networks and the roles that individuals play within them and take greater mitigation and precautionary approaches – in particular through real-time data coming from virtual/human networks, big data analysis, remote observation and crowd-sourced analytics. This should enable states to regulate themselves predominantly within the paradigm of law enforcement without having to resort to the permissive law of armed conflict framework on the use of force – but this will require ongoing dialogue between governments and their intelligence and police services.

A Dangerous Guessing Game?100

This discussion has suggested that in 21st century operating theatres, strategists will have to be highly attuned and adaptive to a broad spectrum of violence which occurs within an complex, cluttered and diffuse information environment which is likely to comprise a diverse range of non-state actors who use a variety of IRCs to further the reach and lethality of their asymmetric strategies and unconventional responses. This global information environment serves to create networked wars without clear spatial or geographical fronts, that may break out in civilianised and urbanised terrain and which are in a constant state of flux. This challenges the ability of our legal and strategic frameworks both to predict and to respond appropriately, and part of the challenge here is to constrain the ambit of conventional military responses which are increasingly being seen to be ineffective and counter-productive in situations of low-intensity violence involving non-state actors who are globally connected.101 The indicative guidelines discussed in this paper may serve to promote to a high threshold of applicability law enforcement and diplomatic lines of state power that are based on human rights and criminal justice, in order that the legal and strategic frameworks of armed conflict are constrained as far as possible within a globalised environment which can quickly expand and escalate an area of operations far beyond those geographical zones where physical effects are created. Intelligence-led approaches involving well- trained, versatile and agile forces that can adjust to a broad spectrum of violence should continue to be developed, and one of their key assets needs to be constantly developing ISTAR capabilities so that they can form an astute situational awareness of threats in any given context, avoid intelligence failures, errors and manipulation, and respond using precise, discriminating and tailored application of effects.102 In part, this requires lawyers, target planners and strategists to engage in the type of social network analysis discussed in this paper, which incorporates indicative guidelines from international criminal law, as a basis for the most effective lines of operations.

References

1 Charles Garraway, '"To Kill or Not to Kill?" – Dilemmas on the Use of Force' (2010) 14 (3)

Journal of Conflict & Security Law, 500–501.

2 UK House of Lords & House of Commons Joint Committee on Human Rights, 'The Government's Policy on the use of Drones for Targeted Killing' (Second Report of Session 2015–2016) (House of Lords and House of Commons Paper, 10 May 2016) paras 1.25 and 1.26.

3 UK House of Commons Defence Committee, 'UK Armed Forces Personnel and the Legal Framework for Future Operations' (Twelfth Report of Session 2013–14) (House of Commons, 2 April 2013), para 129.

4 Kenneth Watkin, 'Stability Operations: A Guiding Framework for "Small Wars" and Other Conflicts of the Twenty-First Century?' in Michael N Schmitt (ed), The War in Afghanistan: A Legal Analysis (US Naval War College Press, 2009) 411, 417.

5 General Charles C Krulak, 'The Strategic Corporal: Leadership in the Three Block War' (January 1999) Marines Magazine.

6 US Joint Chiefs of Staff, Information Operations, Joint Publication 3–13 (27 November 2012 Incorporating Change 1, 20 November 2014).

7 Ibid.

8 Ibid., Chapter I, 1(b), Chapter I, para 2(a).

9 US Department of the Army (Training and Doctrine Command) Counterinsurgency (COIN) Field Manual (FM) 3–24 and Marine Corps War fighting Publication (MCWP) 3–33.5 (Headquarters, Department of the Army, Washington, DC & Marine Corps Combat Development Command, Department of the Navy, Headquarters, United States Marine Corps, Washington, DC 15 December 2006) paras 2–34 and 2–35.

10 FM 3–13, above n 6, Chapter I, para. 2(c). David Kilcullen, Future Land Operational Concept – Complex Warfighting (Report) (The Australian Army, 7 April 2004), 7.

11 FM 3–24, above n 9, paras 2–5.

12 David Ronfeldt, John Arquilla Graham E. Fuller Melissa Fuller, The Zapatista "Social Netwar" in Mexico (Rand, 1998), 9.

13 Jason Burke, The New Threat From Islamic Militancy (Vintage, 2016), 16–22.

14 David Kilcullen, Blood Year: Islamic State and the Failures of the War on Terror (Hurst & Company, London 2016), 120–2.

15 Abdel-Bari Atwan, Islamic State: The Digital Caliphate (Saqi Books, 2015), 1, 2, 9, 10.

16 The Zapatista "Social Netwar" in Mexico, above n 12, 3, 4, 64.

17 Kilcullen, above n 14, 122.

18 David Kilcullen, Out of the Mountains: The Coming Age of the Urban Guerrilla (Hurst & Company, London 2015), vii.

19 FM 3–24, above n 9, paras 2–33 and 2–34.

20 Kilcullen, above n 18, 171–2.

21 Kilcullen, above n 18,16. Kilcullen, above n 10, 5–10, 18–19.

22 FM 3–24, above n 9, paras 2–33, 2–34, 8–6.

23 Kilcullen, above n 14, 198.

24 Kilcullen, above n 10, 18–19.

25 Ibid., 19–20.

26 Ibid.

27 Kilcullen, above n 18, 171–2.

28 Christopher Rogers, Rachel Reid & Chris Kolenda, The Strategic Costs of Civilian Harm – Applying Lessons from Afghanistan to Current and Future Conflicts (Report) (Open Society Foundations – Washington, D.C. June 2016), pp. 18, 19, 22, 23. See also, Akbar Ahmed's, The Thistle and the Drone: How America's War on Terror Became a Global War on Tribal Islam (EDS Publications Ltd. 30 March 2013) and Matthew Hoh's 2009 resignation from his post as a Political Officer in the US Foreign Service and Senior Civilian Representative for the US Government in the Zabul Province of Afghanistan. <http://www.washingtonpost.com/wpsrv/hp/ssi/wpc/ResignationLetter.pdf>.

29 Ibid., Rogers, 19.

30 Elizabeth Wilmshurst, 'Conclusions', in Elizabeth Wilmshurst (ed), International Law and the Classification of Conflicts (OUP 2012), 495.

31 Prosecutor v Lubanga (Judgment pursuant to Article 74 of the Statute) ICC-01/04-01/06 (14

March 2012), 537.

32 Prosecutor v Boškoski and Tarculovski (Trial Judgment) ICTY-04-82-T (10 July 2008), para 177. 33 Ibid.

34 Ibid.

35 Ibid.

36 Ibid.

37 Ibid.

38 Ibid.

39 Ibid.

40 Ibid.

41 Ibid, 178. Kilcullen, above n 10, 17.

42 Ibid.

43 Ibid.

44 United Nations Counter Terrorism Committee, Technical Guide to the Implementation of Security Council Resolution 1373 of 2001 (2009) (Counter-Terrorism Committee Executive Directorate), 27.

45 Ibid.

46 Ariel Zemach, 'The Unpleasant Responsibilities of International Human Rights Law' (2010) 38 Denver Journal of International Law and Policy, 421.

47 Boškoski (Trial Judgment) above n 32, 196; Prosecutor v Slobodan Milošević (Rule 98 bis Decision) IT-02-54-T (16 June 2004), 23; Prosecutor v Limaj et al. (Trial Judgment) ICTY-03- 66-T (30 November 2005), 89.

48 Boškoski. ibid.

49 Jean S Pictet (ed), Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Commentary (International Committee of the Red Cross, Geneva 1960) (Commentary II), 34.

50 Ministère public et Centre pour l'égalité des chances et la lutte contre le racisme v C et B (17 December 1997) Belgian Military Court, Journal des Tribunaux, 4 April 1998, pp. 286–289 (unofficial French translation from the Dutch original ruling) (Violations of IHL in Somalia and Rwanda), 286–289.

51 Boškoski (Trial Judgment) above n 32, 197.

52 Lubanga, above n 31, 537.

53 Boškoski (Trial Judgment) above n 32, 199.

54 Ibid.

55 Ibid, 200.

56 Ibid, 201.

57 Ibid, 202.

58 Ibid, 203.

59 Ibid, 203.

60 FM 3–24, above n 9, para 7.53.

61 Kilcullen, above n 14, 127, 128, 133, 214. Atwan, above n 15, 140–4.

62 FM 3–24, above n 9, paras 10–36.

63 Ibid, paras. 4–79, 4–88.

64 Ibid, paras 4–77.

65 Ibid, paras 4–96.

66 Ibid, paras 4–80.

67 Ibid, paras 4–95.

68 Ibid, paras 4–89 and 4–95.

69 Ibid, paras 4–99.

70 Ibid, paras 4–89.

71 Ibid, paras 4–96.

72 Kilcullen, above n 14, 123.

73 FM 3–24, above n 9, paras 7–53.

74 FM 3–24, above n 9, paras 4–89.

75 Kilcullen, above n 18, 32.

76 Ibid, 34.

77 Ibid, 51.

78 FM 3–24, above n 9, paras 2–36.

79 Kilcullen, above n 18, 203–4.

80 FM 3–24, above n 9, paras 4–100 and 4–102.

81 FM 3–13, above n 6, Chapter 1(a).

82 FM 3–24, above n 9, paras 8–6.

83 Ibid, paras 4–85.

84 Ibid, paras 4–84.

85 Ibid, paras 4–80.

86 Kilcullen, above n 14, 52, 62, 64.

87 Ibid, 90.

88 FM 3–24, above n 9, paras 4–89.

89 Ibid, paras 4–77.

90 FM 3–24, above n 9, paras 4–101, 4–78 and 4–77.

91 Kilcullen, above n 14, 124.

92 FM 3–24, above n 9, paras 4–87.

93 Kilcullen, above n 14, 122.

94 FM 3–24, above n 9, paras 4–97 and 4–98.

95 Kilcullen, above n 14, 202–28.

96 Atwan, above n 15, 4; and Burke above n 13, 206–7.97 Kilcullen, above n 18, 171–2.

98 FM 3–24, above n 9, paras 4–89.

99 FM 3–24, above n 9, paras 4–90.

100 Major Timothy P Bulman, 'A Dangerous Guessing Game Disguised as Enlightened Policy: United States Law of War Obligations During Military Operations Other Than War' (1999) Military Law Review 152, 159.

101 Michel Veuthey, Guérilla et Droit Humanitaire (Institut Henry-Dunant, 1983), 355–356; Nathaniel Berman, 'Privileging Combat? Contemporary Conflict and the Legal Construction of War' (2004) 43(1) Columbia Journal of Transnational Law, 23–24.

102 Kilcullen, above n 10, 6, 9, 17.